Claims

1. A communication system comprising plural general communication apparatuses each holding an old common key before an update and a common key control apparatus that is connected to each general communication apparatus via a certain network and updates the old common key to a new common key, characterized in that:

the common key control apparatus includes,

data transmission processing means for transmitting a first status transition request to all general communication apparatuses having made a transition to a distribution completed status, and transmitting a second status transition request to all the general communication apparatuses when the new common key has been distributed to all the general communication apparatuses, and

each general communication apparatus includes,

transition means for causing a transition to take place from an update completed status to the distribution completed status upon receipt of the new common key from the common key control apparatus, causing a transition to take place from the distribution completed status to the in-transit status upon receipt of the first status transition request, and restoring the status to the update completed status from the in-transit status upon receipt of the second status transition request;

common key holding means for holding a most recent common

key alone during the update completed status, and holding both the old common key and the new common key during the distribution completed status and the in-transit status; and

encryption means for encrypting data using the most recent common key during the update completed status, encrypting transmission data using the old common key during the distribution completed status, and encrypting the transmission data using the new common key during the in-transit status.

2. The communication system according to Claim 1, wherein the common key control apparatus further includes:

common key update means for generating the new common key using a random number.

3. The communication system according to Claim 2, wherein:

the common key update means generates the new common key when the number of encryptions of the transmission data or the number of decryptions of reception data using the old common key exceeds a specific number of times.

4. The communication system according to Claim 2, wherein:

the common key update means generates the new common key

when a sum of the number of encryptions of the transmission data and the number of decryptions of reception data using the old common key exceeds a specific number of times.

5. The communication system according to Claim 2, wherein:

the common key update means generates the new common key when a specific time has passed as a use period of the old common key.

6. The communication system according to any one of Claims 1 through 5, wherein:

the common key holding means holds a history of common keys transmitted to the general communication apparatuses, and holds a management table that stores respective transmitted common keys in correlation with general communication apparatus information containing addresses of the general communication apparatuses to which the respective common keys are transmitted.

7. A common key control apparatus according to Claim 6, wherein:

when data is received from a general communication apparatus whose general communication apparatus information is not stored in the management table, the common key update

means generates the new common key and updates common keys held in the general communication apparatuses whose general communication information is stored in the management table to the new common key.

8. The communication system according to any one of Claims 1 through 7, wherein:

the common key control apparatus further includes initial common key input means for inputting an initial common key held in the general communication apparatus when the general communication apparatus is linked to the network.

9. The communication system according to Claim 8, wherein:

the initial common key input means includes at least one of a keyboard, a touch panel, and a mouse.

10. The communication system according to Claim 8, wherein:

the initial common key input means includes a remote controller of the general communication apparatus holding the initial common key and a light-receiving portion that receives a signal from the remote controller.

11. The communication system according to Claim 8,

wherein:

the initial common key input means is a code reading device.

12. The communication system according to Claim 8, wherein:

the initial common key input means is a storage medium driving device.

13. The communication system according to any one of Claims 1 through 12, wherein:

each general communication apparatus further includes common key request means for generating data requesting the common key control apparatus to transmit the new common key, and transmitting the data to the common key control apparatus when a communication disabled state is changed to a communication enabled state.

14. The communication system according to any one of Claims 1 through 13, wherein:

each general communication apparatus further includes decryption means for determining which of the old common key and the new common key was used for encryption of reception data by trying to decrypt the reception data using the old common key and the new common key while its own apparatus is

in the distribution completed status.

15. The communication system according to Claim 14, wherein:

the decryption means determines which of the old common key and the new common key was used for encryption of the reception data by trying to decrypt the reception data using the old common key and the new common key while its own apparatus in the in-transit status.

16. The communication system according to Claim 14 or 15, wherein:

the decryption means decrypts the reception data using the most recent common key while its own apparatus is in the update completed status.

17. A general communication apparatus connected via a communication network to a common key control apparatus that transmits a first status transition request to all general communication apparatuses having made a transition to a distribution completed status and transmits a second status transition request to all the general communication apparatuses when a new common key has been distributed to all the general communication apparatuses including:

transition means for causing a transition to take place

from an update completed status to the distribution completed status upon receipt of the new common key from the common key control apparatus, causing a transition to take place from the distribution completed status to the in-transit status upon receipt of the first status transition request, and restoring the status to the update completed status from the in-transit status upon receipt of the second status transition request;

common key holding means for holding a most recent common key alone during the update completed status, and holding both the old common key and the new common key during the distribution completed status and the in-transit status; and

encryption means for encrypting transmission data using the most recent common key during the update completed status, encrypting the transmission data using the old common key during the distribution completed status, and encrypting the transmission data using the new common key during the in-transit status.

18. A common key control apparatus connected to plural general communication apparatuses via a communication network,

each general communication apparatus including:

transition means for causing a transition to take place from an update completed status to a distribution completed status upon receipt of a new common key from the common key

control apparatus, causing a transition to take place from the distribution completed status to an in-transit status upon receipt of a first status transition request from the common key control apparatus, and restoring the status to the update completed status from the in-transit status upon receipt of a second status transition request from the common key control apparatus;

common key holding means for holding a most recent common key alone during the update completed status, and holding both the old common key and the new common key during the distribution completed status and the in-transit status; and

encryption means for encrypting transmission data using the most recent common key during the update completed status, encrypting the transmission data using the old common key during the distribution completed status, and encrypting the transmission data using the new common key during the in-transit status,

the common key control apparatus being characterized in that the common key control apparatus transmits the first status transition request to all general communication apparatuses from which a new common key update reply has been transmitted after a new common key update request was transmitted to all the general communication apparatuses, and transmits the second status transition request to all the general communication apparatuses when the new common key has

been distributed to all the general communication apparatuses.